jhn

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/772,451	01/29/2001	David Yin-Shur Ma	CLAR-0200	2593

7590 05/03/2005

David R. Stevens
Stevens & Westberg LLP
Suite 201
99 North First Street
San Jose, CA 95113

EXAMINER	
CHOUDHURY, AZIZUL Q	
ART UNIT	**PAPER NUMBER**
2145	

DATE MAILED: 05/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/772,451	MA ET AL.	
	Examiner	Art Unit	
	Azizul Choudhury	2145	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 December 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 January 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Detailed Action

This office action is in response to the correspondence received on December 13, 2004.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Szymansky (US Pat No: US006557029B2) in view of Shani (US Pat No: US006363482B1).

1. With regards to claim 1, Szymansky teaches through Shani for use in a communication interface for communication between a wireless device and the communication interface, the communication interface being configured to communicate with other devices communicating with a network and configured to facilitate data communication between the wireless device and other devices connected to the network, where the network is configured under a network protocol that requires all network devices receive and send data packets related to administrative procedures within the network, such as device naming protocols, a computer readable medium having stored thereon a plurality of sequences of instructions, said sequences of

instructions including instructions that, when executed by a processor, cause said processor to perform the steps of receiving an initialization packet from a wireless device indicating whether the signal carrying the message is configured under a first protocol; establishing a communication link with the wireless device; establishing another communication link between the wireless device and the network; and managing the transmission to the wireless device of authorized communication signals sent from the computer system by: receiving and analyzing signals when received; determining whether the signals received from the network are directed to the wireless device; if they are directed to the wireless device, screening the messages to determine whether they are configured under a first protocol to prevent unauthorized signal transmissions to the wireless device; and if the messages are directed to the wireless device and are also configured under the first protocol, then transmitting authorized signals to the wireless device according to the first communication protocol

(The claimed steps of initialization packets being received and establishing communication links are obvious steps within networks, especially wireless networks. Such steps are detailed within the protocols and Szymansky's design allows for a variety of protocols (column 3, lines 40-43, Szymansky). Szymansky teaches a design that uses a PDA to wirelessly communicate with a computer server that communicates with a network (column 2, lines 15-23, Szymansky). In addition, as in all networks, the transmissions to the wireless device are managed and the wireless client is authorized to communicate with the network as claimed (column 4, lines 10-18, Szymansky).

However while it is known that wireless data paths are insecure compared to wire data paths, Szymansky's design does not teach it.

Shani's disclosure teaches network designs. In the design, Shani discloses that wireless data transmission leaves data transmissions vulnerable (column 1, lines 36-40, Shani). Hence, it is obvious to not transmit important data (i.e. administrative data) through wireless transmissions as claimed.

Both Szymansky's and Shani's disclosures teach about wireless networks. While Szymansky's design allows for wireless networks with authorization, it does not teach the vulnerabilities of wireless networks. Shani's disclosure teaches such vulnerabilities making it obvious not to transmit sensitive data over a wireless network. Therefore, it would have been obvious to one skilled in the art, during the time of the invention, to have combined the teachings of Szymansky with those of Shani, for the purpose of ensuring important data is secure).

2. With regards to claim 2, Szymansky teaches through Shani, a method wherein the managing of the transmission includes: examining data packets transferred between a wireless device and a network device; determining which signals are authorized for transmission to the wireless device according to a first communication protocol; and if the examination of a data packet indicates that the wireless device has authorized the transmission of authorized communications to the wireless device, transmitting a data packet to the wireless device if the examination of a data packet

indicates that the wireless device has not authorized the transmission of authorized communications to the wireless device, not transmitting a data packet to the wireless device; and if the examination of a data packet indicates that the transmissions directed to the wireless device are related to administrative functions of the transmitting network that do not relate to the transmission of data to the wireless device, not transmitting a data packet to the wireless device

(Szymansky's design has a wireless PDA (wireless device) communicate with a network (column 2, lines 15-23, Szymansky). The data in this network, as in all networks is transferred in packets (column 3, line 52, Szymansky). Szymansky's design manages the data transfers and takes steps to ensure the authenticity of the PDA (wireless device client) (column 4, lines 10-18, Szymansky). In addition, Szymansky's design takes steps to check the logins of the users and ensure the security of the data transmissions (claim 11, Szymansky). However while it is known that wireless data paths are insecure compared to wire data paths, Szymansky's design does not teach it.

Shani's disclosure teaches network designs. In the design, Shani discloses that wireless data transmission leaves data transmissions vulnerable (column 1, lines 36-40, Shani). Hence, it is obvious to not transmit important data (i.e. administrative data) through wireless transmissions as claimed.

Both Szymansky's and Shani's disclosures teach about wireless networks. While Szymansky's design allows for wireless networks with authorization, it does not teach the vulnerabilities of wireless networks. Shani's disclosure teaches such vulnerabilities making it obvious not to transmit sensitive data over a wireless network. Therefore, it

would have been obvious to one skilled in the art, during the time of the invention, to have combined the teachings of Szymansky with those of Shani, for the purpose of ensuring important data is secure).

3. With regards to claim 3, Szymansky teaches through Shani, a method wherein the managing of the transmission includes: examining a data packet transferred between a wireless device and a network device; determining whether the data packet is authorized for transmission to the wireless device according to a first communication protocol, wherein properties of the first protocol include refraining from transmitting data packets that pertain to administrative operations of the network that are not necessary for the transmission of data packets to the wireless device; and if the examination of a data packet indicates that the wireless device has authorized the transmission of particular communications to the wireless device, transmitting a data packet to the wireless device; if the examination of a data packet indicates that the wireless device has not authorized the transmission of particular communications to the wireless device, not transmitting a data packet to the wireless device

(The steps of examining data packets is obvious in networks. Szymansky's design manages the data transfers and takes steps to ensure the authenticity of the PDA (wireless device client) (column 4, lines 10-18, Szymansky). In addition, Szymansky's design takes steps to check the logins of the users and ensure the security of the data transmissions (claim 11, Szymansky). However while it is known

that wireless data paths are insecure compared to wire data paths, Szymansky's design does not teach it.

Shani's disclosure teaches network designs. In the design, Shani discloses that wireless data transmission leaves data transmissions vulnerable (column 1, lines 36-40, Shani). Hence, it is obvious to not transmit important data (i.e. administrative data) through wireless transmissions as claimed.

Both Szymansky's and Shani's disclosures teach about wireless networks. While Szymansky's design allows for wireless networks with authorization, it does not teach the vulnerabilities of wireless networks. Shani's disclosure teaches such vulnerabilities making it obvious not to transmit sensitive data over a wireless network. Therefore, it would have been obvious to one skilled in the art, during the time of the invention, to have combined the teachings of Szymansky with those of Shani, for the purpose of ensuring important data is secure).

4. With regards to claim 4, Szymansky teaches through Shani, a method wherein the managing of the transmission includes: examining a data packet transferred between a wireless device and a network device; determining whether the wireless device is configured to communicate under a first protocol, wherein the first protocol dictates whether a data packet is authorized for transmission to the wireless device, and wherein the first protocol screens administrative data packets to prevent transmissions to the wireless device that are not necessary to the transmission of data packets to wireless devices; and if the examination of a data packet indicates that the wireless

device is configured under the first protocol, transmitting a data packet to the wireless device; if the examination of a data packet indicates that the wireless device is not configured under the first protocol, not transmitting a data packet to the wireless device

(The steps of examining data packets is obvious in networks. Szymansky's design manages the data transfers and takes steps to ensure the authenticity of the PDA (wireless device client) (column 4, lines 10-18, Szymansky). In addition, Szymansky's design takes steps to check the logins of the users and ensure the security of the data transmissions (claim 11, Szymansky). If the security is unable to be authenticated, it is obvious that the data will cease to be transmitted. As for protocol configuration, all networks abide by protocols. When communications are first established, the determination of the protocol is one of the first steps to occur since it sets the rules by which data is to be transferred. Hence the claimed features must be present within Szymansky's design. However while it is known that wireless data paths are insecure compared to wire data paths, Szymansky's design does not teach it.

Shani's disclosure teaches network designs. In the design, Shani discloses that wireless data transmission leaves data transmissions vulnerable (column 1, lines 36-40, Shani). Hence, it is obvious to not transmit important data (i.e. administrative data) through wireless transmissions as claimed.

Both Szymansky's and Shani's disclosures teach about wireless networks. While Szymansky's design allows for wireless networks with authorization, it does not teach the vulnerabilities of wireless networks. Shani's disclosure teaches such vulnerabilities making it obvious not to transmit sensitive data over a wireless network. Therefore, it

would have been obvious to one skilled in the art, during the time of the invention, to have combined the teachings of Szymansky with those of Shani, for the purpose of ensuring important data is secure).

5. With regards to claim 5, Szymansky teaches through Shani for use in a communication interface for communication between a wireless device and another device via the communication interface, the communication interface being configured to communicate with other devices communicating with a network and configured to facilitate data communication between the wireless device and other devices connected to the network and to filter out certain communications from reaching the wireless device, where the network is configured under a network protocol that requires all network devices receive and send data packets related to administrative procedures within the network, such as device naming protocols, a computer readable medium having stored thereon a plurality of sequences of instructions, said sequences of instructions including instructions that, when executed by a processor, cause said processor to perform the steps of: receiving a data packet transmission between a network affiliated device and a wireless device; analyzing the data packet when received: determining whether the data packet contents indicate whether the wireless device is configured to accept session data packets from a network device; if the wireless device is configured to accept session data packets related to transmitting data packets other than those related to administrative operations of the network from a network device, transmitting session data packets to the wireless device

(The steps of examining data packets are obvious in networks. Szymansky's design manages the data transfers and takes steps to ensure the authenticity of the PDA (wireless device client) (column 4, lines 10-18, Szymansky). In addition, Szymansky's design takes steps to check the logins of the users and ensure the security of the data transmissions (claim 11, Szymansky). Furthermore, it is also obvious that devices are checked (polled) to verify that they are able to communicate (accept data packets) in a network during the initialization of communications as claimed. However while it is known that wireless data paths are insecure compared to wire data paths, Szymansky's design does not teach it.

Shani's disclosure teaches network designs. In the design, Shani discloses that wireless data transmission leaves data transmissions vulnerable (column 1, lines 36-40, Shani). Hence, it is obvious to not transmit important data (i.e. administrative data) through wireless transmissions as claimed.

Both Szymansky's and Shani's disclosures teach about wireless networks. While Szymansky's design allows for wireless networks with authorization, it does not teach the vulnerabilities of wireless networks. Shani's disclosure teaches such vulnerabilities making it obvious not to transmit sensitive data over a wireless network. Therefore, it would have been obvious to one skilled in the art, during the time of the invention, to have combined the teachings of Szymansky with those of Shani, for the purpose of ensuring important data is secure).

6. With regards to claim 6, Szymansky teaches through Shani, a method wherein the communication interface determines whether a wireless device is configured to receive Windows network communications protocol by: examining data packets transmitted from the wireless device to the network device; if the data packet does not include an indicia for administrative process of the Windows™ network that may be used to identify the wireless device as a Windows™ network compliant device by performing Windows™ renaming operations, filtering Windows™ network protocol data packets from transmission to the wireless device; and if the data packet does not include any indicia that may be used to identify the wireless device as a Windows™ network compliant device, allowing Windows™ network protocol data packets to be transmitted to the wireless device

(The claimed steps primarily focus on having devices determine what protocols are acceptable within the network and using the protocols that are allowed. Such traits are present within data networks. Devices obviously must check for the protocols being used if they are network-enabled devices, as they are in Szymansky's design. Furthermore, Szymansky goes on to state that the design allows for a device to send data from one network to a device in second network. Plus, Szymansky's design permits the use of various different protocols (column 3, lines 36-44, Szymansky). However while it is known that wireless data paths are insecure compared to wire data paths, Szymansky's design does not teach it.

Shani's disclosure teaches network designs. In the design, Shani discloses that wireless data transmission leaves data transmissions vulnerable (column 1, lines 36-40,

Shani). Hence, it is obvious to not transmit important data (i.e. administrative data) through wireless transmissions as claimed.

Both Szymansky's and Shani's disclosures teach about wireless networks. While Szymansky's design allows for wireless networks with authorization, it does not teach the vulnerabilities of wireless networks. Shani's disclosure teaches such vulnerabilities making it obvious not to transmit sensitive data over a wireless network. Therefore, it would have been obvious to one skilled in the art, during the time of the invention, to have combined the teachings of Szymansky with those of Shani, for the purpose of ensuring important data is secure).

7. With regards to claim 7, Szymansky teaches through Shani for use in a communication interface for communication between a personal data assistant (PDA) and the communication interface, the communication interface being configured to communicate with other devices communicating with the internet and configured to facilitate data communication between the PDA and other devices, where the network is configured under a network protocol that requires all network devices receive and send data packets related to administrative procedures within the Internet network, such as device naming protocols, a computer readable medium having stored thereon a plurality of sequences of instructions, said sequences of instructions including instructions that, when executed by a processor, cause said processor to perform the steps of receiving an initiation packet from a computer system that is intended to be broadcast to devices outside the network; receiving communications signals from devices outside the

network that identify outside devices; determining which outside devices are configured as network devices by; (1) transmitting network related administrative data packets to the outside devices; and (2) analyzing the communication signals sent by such devices that are capable of communication with devices associated with the network; sending the broadcast initiation packet to outside devices that are identified as network devices; and filtering the broadcast initiation packet from outside devices that are identified as PDA devices to prevent the broadcast initiation packet from being transmitted to the PDA

(It is obvious that devices are checked (polled) to verify that they are able to communicate (accept data packets) in a network during the initialization of communications as claimed. As for broadcasting initialization packets, this too is obvious in wireless networks since the actual location of the wireless client device is unknown prior to initialization. However while it is known that wireless data paths are insecure compared to wire data paths, Szymansky's design does not teach it.

Shani's disclosure teaches network designs. In the design, Shani discloses that wireless data transmission leaves data transmissions vulnerable (column 1, lines 36-40, Shani). Hence, it is obvious to not transmit important data (i.e. administrative data) through wireless transmissions as claimed.

Both Szymansky's and Shani's disclosures teach about wireless networks. While Szymansky's design allows for wireless networks with authorization, it does not teach the vulnerabilities of wireless networks. Shani's disclosure teaches such vulnerabilities making it obvious not to transmit sensitive data over a wireless network. Therefore, it

would have been obvious to one skilled in the art, during the time of the invention, to have combined the teachings of Szymansky with those of Shani, for the purpose of ensuring important data is secure).

8. With regards to claim 8, Szymansky teaches through Shani, a communication interface for managing communication between a wireless device and a network device comprising: a receiver configured to receive data packets received by the communication device, the receiver including a signal receiver configured to receive a signal used for transmitting data over a medium and converter configured to convert the data signal into a form that can be stored; a transmitter configured to transmit data packets over a medium; a storage device configured to store data, the storage device including a storage mechanism for storing data packets received by the receiver; an analyzer configured to examine data packets transmitted between a wireless device and a network device, where the network is configured under a network protocol that requires all network devices receive and send data packets related to administrative device naming procedures within the network; and a filter mechanism configured manage data transmissions between the wireless device and the network device by filtering out data packets related to administrative device naming procedures within the network

(Szymansky teaches a design that uses a PDA to wirelessly communicate with a computer server that communicates with a network (column 2, lines 15-23, Szymansky). In addition, as in all networks, the transmissions to the wireless device are managed (as

done by the filter mechanism in the claim) and the wireless client is authorized to communicate with the network as claimed (column 4, lines 10-18, Szymansky). Since data is transferred wirelessly, the presence of receivers and transmitters as claimed must obviously be present. Furthermore, Szymansky's design uses computers and PDAs, both of which have storage means. Finally, data packets are obviously analyzed in networks. However while it is known that wireless data paths are insecure compared to wire data paths, Szymansky's design does not teach it.

Shani's disclosure teaches network designs. In the design, Shani discloses that wireless data transmission leaves data transmissions vulnerable (column 1, lines 36-40, Shani). Hence, it is obvious to not transmit important data (i.e. administrative data) through wireless transmissions as claimed.

Both Szymansky's and Shani's disclosures teach about wireless networks. While Szymansky's design allows for wireless networks with authorization, it does not teach the vulnerabilities of wireless networks. Shani's disclosure teaches such vulnerabilities making it obvious not to transmit sensitive data over a wireless network. Therefore, it would have been obvious to one skilled in the art, during the time of the invention, to have combined the teachings of Szymansky with those of Shani, for the purpose of ensuring important data is secure).

9. With regards to claim 9, Szymansky teaches through Shani, a communication interface, wherein the analyzer includes an identifier that is configured to identify a data packet sent by a particular wireless device that is configured according to a first

protocol, and wherein the filter mechanism is configured to subsequently relay data packets that are sent by a network device that are configured according to the first protocol to the particular wireless device in response to the analyzer receiving a data packet sent by the particular wireless device to prevent data packets related to network renaming procedures from being sent to the wireless device

(All data packets have header information that provides information such as the intended recipient. Furthermore, all the claimed features are performed in networks by routers and Szymansky's design uses routers (column 3, line 29, Szymansky). However while it is known that wireless data paths are insecure compared to wire data paths, Szymansky's design does not teach it.

Shani's disclosure teaches network designs. In the design, Shani discloses that wireless data transmission leaves data transmissions vulnerable (column 1, lines 36-40, Shani). Hence, it is obvious to not transmit important data (i.e. administrative data) through wireless transmissions as claimed.

Both Szymansky's and Shani's disclosures teach about wireless networks. While Szymansky's design allows for wireless networks with authorization, it does not teach the vulnerabilities of wireless networks. Shani's disclosure teaches such vulnerabilities making it obvious not to transmit sensitive data over a wireless network. Therefore, it would have been obvious to one skilled in the art, during the time of the invention, to have combined the teachings of Szymansky with those of Shani, for the purpose of ensuring important data is secure).

10. With regards to claim 10, Szymansky teaches through Shani, a communication interface, wherein the analyzer is configured to identify a data packet sent by a wireless device that is configured according to a first protocol that refrains from transmitting packets related to network naming protocols used by the network to name devices authorized to communicate with other devices connected to the network, and wherein the filter mechanism is configured to subsequently relay data packets to the wireless device that are sent by a network device and that are configured according to the first protocol by preventing unnecessary data packet transmissions to the wireless device

(As stated earlier, all data packets have header information which provides information such as the intended recipient. Furthermore, all the claimed features are performed in networks by routers and Szymansky's design uses routers (column 3, line 29, Szymansky). However while it is known that wireless data paths are insecure compared to wire data paths, Szymansky's design does not teach it.

Shani's disclosure teaches network designs. In the design, Shani discloses that wireless data transmission leaves data transmissions vulnerable (column 1, lines 36-40, Shani). Hence, it is obvious to not transmit important data (i.e. administrative data) through wireless transmissions as claimed.

Both Szymansky's and Shani's disclosures teach about wireless networks. While Szymansky's design allows for wireless networks with authorization, it does not teach the vulnerabilities of wireless networks. Shani's disclosure teaches such vulnerabilities making it obvious not to transmit sensitive data over a wireless network. Therefore, it would have been obvious to one skilled in the art, during the time of the invention, to

have combined the teachings of Szymansky with those of Shani, for the purpose of ensuring important data is secure).

11. With regards to claim 11, Szymansky teaches through Shani, a communication interface, wherein the analyzer includes an identifier that is configured to identify a data packet transmitted by a wireless device that indicates that the transmitting wireless device is configured according to a first protocol that permits transmission to devices that are not subject to naming protocols within the network by transmitting data via a network interface, and wherein the filter mechanism is configured to subsequently relay data packets that are sent by a network device that are configured according to the first protocol only to wireless devices that have transmitted such a packet having such indicia

(As stated earlier, all data packets have header information that provides information such as the intended recipient. Furthermore, the claimed features concerning filtering and transmission of data are performed in networks by routers and Szymansky's design uses routers (column 3, line 29, Szymansky). However while it is known that wireless data paths are insecure compared to wire data paths, Szymansky's design does not teach it.

Shani's disclosure teaches network designs. In the design, Shani discloses that wireless data transmission leaves data transmissions vulnerable (column 1, lines 36-40, Shani). Hence, it is obvious to not transmit important data (i.e. administrative data) through wireless transmissions as claimed.

Both Szymansky's and Shani's disclosures teach about wireless networks. While Szymansky's design allows for wireless networks with authorization, it does not teach the vulnerabilities of wireless networks. Shani's disclosure teaches such vulnerabilities making it obvious not to transmit sensitive data over a wireless network. Therefore, it would have been obvious to one skilled in the art, during the time of the invention, to have combined the teachings of Szymansky with those of Shani, for the purpose of ensuring important data is secure).

12. With regards to claim 12, Szymansky teaches through Shani, a communication interface for affecting communication between a wireless device and a network device comprising: receiver means for receiving data packets; converter means for converting the data signal into a form that can be stored; transmission means for transmitting data packets over a medium; storage means for storing data packets; examining means for examining data packets transmitted between a wireless device and a network device to determine whether data packets are directed to transmitting administrative renaming queries to devices connected to the network; and filter means for filtering our data transmissions between the wireless device and the network device upon a condition, where administrative renaming procedures are prevented from being transmitted to a wireless device

(Szymansky discloses a design where data is transferred between devices in a network (column 2, lines 15-23, Szymansky). As in all networks, receiving and transmission means must obviously be present since data is transferred. In addition,

Szymansky's design uses computers and PDAs and they obviously have storage means (column 2, lines 15-23, Szymansky). As for converting data before storage, this is done to all data in all computing systems. Plus, all networks examine data packets. Additionally, data in all computing systems must be converted before it is stored as claimed. Finally, as for the filtering means, Szymansky's design has steps on user authentication (column 4, lines 10-18, Szymansky) and for data transmission authentication (claim 11, Szymansky). It is therefore obvious that filtering means, such those claimed are present within Szymansky's design. However while it is known that wireless data paths are insecure compared to wire data paths, Szymansky's design does not teach it.

Shani's disclosure teaches network designs. In the design, Shani discloses that wireless data transmission leaves data transmissions vulnerable (column 1, lines 36-40, Shani). Hence, it is obvious to not transmit important data (i.e. administrative data) through wireless transmissions as claimed.

Both Szymansky's and Shani's disclosures teach about wireless networks. While Szymansky's design allows for wireless networks with authorization, it does not teach the vulnerabilities of wireless networks. Shani's disclosure teaches such vulnerabilities making it obvious not to transmit sensitive data over a wireless network. Therefore, it would have been obvious to one skilled in the art, during the time of the invention, to have combined the teachings of Szymansky with those of Shani, for the purpose of ensuring important data is secure).

13. With regards to claim 13, Szymansky teaches through Shani, a communication interface, wherein the examining means is configured to identify a data packet configured according to a first protocol that is transmitted by the wireless device, and wherein the filter means is configured to subsequently relay data packets that are sent by a network device and that are configured according to the first protocol to the particular wireless device in response to the examining means transmitting a data packet sent by the wireless device, wherein the examining means prevents data packets related to network renaming procedures to the wireless device

(All data packets have header information that provides information such as the intended recipient. Furthermore, the claimed features concerning data routing are performed in networks by routers and Szymansky's design uses routers (column 3, line 29, Szymansky). However while it is known that wireless data paths are insecure compared to wire data paths, Szymansky's design does not teach it.

Shani's disclosure teaches network designs. In the design, Shani discloses that wireless data transmission leaves data transmissions vulnerable (column 1, lines 36-40, Shani). Hence, it is obvious to not transmit important data (i.e. administrative data) through wireless transmissions as claimed.

Both Szymansky's and Shani's disclosures teach about wireless networks. While Szymansky's design allows for wireless networks with authorization, it does not teach the vulnerabilities of wireless networks. Shani's disclosure teaches such vulnerabilities making it obvious not to transmit sensitive data over a wireless network. Therefore, it would have been obvious to one skilled in the art, during the time of the invention, to

have combined the teachings of Szymansky with those of Shani, for the purpose of ensuring important data is secure).

14. With regards to claim 14, Szymansky teaches through Shani, a communication interface, wherein the examining means is configured to identify a data packet sent by a wireless device that is configured according to a first protocol, and wherein the filter means is configured to subsequently relay data packets to the wireless device that are sent by a network device and that are configured according to the first protocol, wherein the examining means prevents data packets related to network renaming procedures to the wireless device according to the first protocol

(As stated earlier, all data packets have header information that provides information such as the intended recipient. Furthermore, the claimed features concerning routing data are performed in networks by routers and Szymansky's design uses routers (column 3, line 29, Szymansky). However while it is known that wireless data paths are insecure compared to wire data paths, Szymansky's design does not teach it.

Shani's disclosure teaches network designs. In the design, Shani discloses that wireless data transmission leaves data transmissions vulnerable (column 1, lines 36-40, Shani). Hence, it is obvious to not transmit important data (i.e. administrative data) through wireless transmissions as claimed.

Both Szymansky's and Shani's disclosures teach about wireless networks. While Szymansky's design allows for wireless networks with authorization, it does not teach

the vulnerabilities of wireless networks. Shani's disclosure teaches such vulnerabilities making it obvious not to transmit sensitive data over a wireless network. Therefore, it would have been obvious to one skilled in the art, during the time of the invention, to have combined the teachings of Szymansky with those of Shani, for the purpose of ensuring important data is secure).

15. With regards to claim 15, Szymansky teaches through Shani, a communication interface, wherein the examining means is configured to identify a data packet transmitted by a wireless device that indicates that the transmitting wireless device is configured according to a first protocol, and wherein the filter means is configured to subsequently relay data packets that are sent by a network device that are configured according to the first protocol only to wireless devices that have transmitted such a packet having such indicia, wherein the indicia alerts the examining means to prevent data packets related to network renaming procedures to the wireless device

(As stated earlier, all data packets have header information which provides information such as the intended recipient. Furthermore, the claimed features concerning routing and filtering are performed in networks by routers and Szymansky's design uses routers (column 3, line 29, Szymansky). However while it is known that wireless data paths are insecure compared to wire data paths, Szymansky's design does not teach it.

Shani's disclosure teaches network designs. In the design, Shani discloses that wireless data transmission leaves data transmissions vulnerable (column 1, lines 36-40,

Shani). Hence, it is obvious to not transmit important data (i.e. administrative data) through wireless transmissions as claimed.

Both Szymansky's and Shani's disclosures teach about wireless networks. While Szymansky's design allows for wireless networks with authorization, it does not teach the vulnerabilities of wireless networks. Shani's disclosure teaches such vulnerabilities making it obvious not to transmit sensitive data over a wireless network. Therefore, it would have been obvious to one skilled in the art, during the time of the invention, to have combined the teachings of Szymansky with those of Shani, for the purpose of ensuring important data is secure).

16. With regards to claim 16, Szymansky teaches through Shani, a system for communicating between a wireless device and a network device comprising: an electronic wireless device configured to communicate with other electronic devices according to a communication protocol; an electronic network device configured to communicate with other electronic devices via a computer network; a communication interface having a receiver configured to receive data packets, the receiver including a signal receiver configured to receive a signal over a transmission medium and a converter configured to convert the data signal into a form that can be stored; a transmitter configured to transmit data packets over a medium; a storage device configured to store data, the storage device including a storage mechanism for storing data packets received by the receiver; an analyzer configured to examine data packets transmitted between the wireless device and the network device to determine whether

the data packets relate to unnecessary administrative procedures related to the operation of the network; and a filter mechanism configured manage data transmissions between the wireless device and the network device and to prevent data packets related to network renaming procedures from being sent to the wireless device

(Szymansky discloses a design where data is transferred between devices in a network (column 2, lines 15-23, Szymansky). As in all networks, receiving and transmission means must obviously be present since data is transferred. In addition, Szymansky's design uses computers and PDAs and they obviously have storage means (column 2, lines 15-23, Szymansky). As for converting data before storage, this is done in all data in all computing systems. Plus, all networks examine data packets. Additionally, data in all computing systems must be converted before it is stored as claimed. Finally, as for the filtering means, Szymansky's design has steps on user authentication (column 4, lines 10-18, Szymansky) and for data transmission authentication (claim 11, Szymansky). It is therefore obvious that filtering means, such those claimed are present within Szymansky's design. However while it is known that wireless data paths are insecure compared to wire data paths, Szymansky's design does not teach it.

Shani's disclosure teaches network designs. In the design, Shani discloses that wireless data transmission leaves data transmissions vulnerable (column 1, lines 36-40, Shani). Hence, it is obvious to not transmit important data (i.e. administrative data) through wireless transmissions as claimed.

Both Szymansky's and Shani's disclosures teach about wireless networks. While Szymansky's design allows for wireless networks with authorization, it does not teach the vulnerabilities of wireless networks. Shani's disclosure teaches such vulnerabilities making it obvious not to transmit sensitive data over a wireless network. Therefore, it would have been obvious to one skilled in the art, during the time of the invention, to have combined the teachings of Szymansky with those of Shani, for the purpose of ensuring important data is secure).

17. With regards to claim 17, Szymansky teaches through Shani, a communication interface, wherein the analyzer includes an identifier that is configured to identify a data packet sent by a particular wireless device that is configured according to a first protocol, and wherein the filter mechanism is configured to subsequently relay data packets that are sent by a network device that are configured according to the first protocol that causes data packets related to network renaming procedures to be prevented from being sent to the wireless device to the particular wireless device in response to the analyzer receiving a data packet sent by the particular wireless device

(All data packets have header information that provides information such as the intended recipient. Furthermore, the claimed features are performed in networks by routers and Szymansky's design uses routers (column 3, line 29, Szymansky). However while it is known that wireless data paths are insecure compared to wire data paths, Szymansky's design does not teach it.

Shani's disclosure teaches network designs. In the design, Shani discloses that wireless data transmission leaves data transmissions vulnerable (column 1, lines 36-40, Shani). Hence, it is obvious to not transmit important data (i.e. administrative data) through wireless transmissions as claimed.

Both Szymansky's and Shani's disclosures teach about wireless networks. While Szymansky's design allows for wireless networks with authorization, it does not teach the vulnerabilities of wireless networks. Shani's disclosure teaches such vulnerabilities making it obvious not to transmit sensitive data over a wireless network. Therefore, it would have been obvious to one skilled in the art, during the time of the invention, to have combined the teachings of Szymansky with those of Shani, for the purpose of ensuring important data is secure).

18. With regards to claim 18, Szymansky teaches through Shani, a communication interface wherein the analyzer is configured to identify a data packet sent by a wireless device that is configured according to a first protocol, and wherein the filter mechanism is configured to subsequently relay data packets to the wireless device that are sent by a network device and that are configured according to the first protocol that prevents data packets related to network renaming procedures from being sent to the wireless device

(As previously stated, all data packets have header information that provides information such as the intended recipient. Furthermore, the claimed features are performed in networks by routers and Szymansky's design uses routers (column 3, line

29, Szymansky). However while it is known that wireless data paths are insecure compared to wire data paths, Szymansky's design does not teach it.

Shani's disclosure teaches network designs. In the design, Shani discloses that wireless data transmission leaves data transmissions vulnerable (column 1, lines 36-40, Shani). Hence, it is obvious to not transmit important data (i.e. administrative data) through wireless transmissions as claimed.

Both Szymansky's and Shani's disclosures teach about wireless networks. While Szymansky's design allows for wireless networks with authorization, it does not teach the vulnerabilities of wireless networks. Shani's disclosure teaches such vulnerabilities making it obvious not to transmit sensitive data over a wireless network. Therefore, it would have been obvious to one skilled in the art, during the time of the invention, to have combined the teachings of Szymansky with those of Shani, for the purpose of ensuring important data is secure).

19. With regards to claim 19, Szymansky teaches through Shani, a communication interface wherein the analyzer includes an identifier that is configured to identify a data packet transmitted by a wireless device that indicates that the transmitting wireless device is configured according to a first protocol, and wherein the filter mechanism is configured to subsequently relay data packets that are sent by a network device that are configured according to the first protocol only to wireless devices that have transmitted such a packet having such indicia to prevent data packets related to network renaming procedures from being sent to the wireless device

(As previously stated, all data packets have header information which provides information such as the intended recipient. Furthermore, the claimed features are performed in networks by routers and Szymansky's design uses routers (column 3, line 29, Szymansky). However while it is known that wireless data paths are insecure compared to wire data paths, Szymansky's design does not teach it.

Shani's disclosure teaches network designs. In the design, Shani discloses that wireless data transmission leaves data transmissions vulnerable (column 1, lines 36-40, Shani). Hence, it is obvious to not transmit important data (i.e. administrative data) through wireless transmissions as claimed.

Both Szymansky's and Shani's disclosures teach about wireless networks. While Szymansky's design allows for wireless networks with authorization, it does not teach the vulnerabilities of wireless networks. Shani's disclosure teaches such vulnerabilities making it obvious not to transmit sensitive data over a wireless network. Therefore, it would have been obvious to one skilled in the art, during the time of the invention, to have combined the teachings of Szymansky with those of Shani, for the purpose of ensuring important data is secure).

Remarks

The amendments and remarks received on December 13, 2004 have been carefully reviewed but are not deemed fully persuasive. For clarification purposes, the examiner is providing responses to the remarks submitted, below.

With regards to the remark that the Szymansky prior art does not disclose the use of any one particular protocol, the examiner agrees. The applicant's representative believes that the lack of a single designated protocol is a weakness of the Szymansky disclosure when used as a prior art against the claimed invention. The examiner feels that by not limiting the type of protocol used, the Szymansky design is able to adjust and provide for the various needs of its users. The protocol traits disclosed within the claims were general traits that are commonly found in most currently known protocols. The examiner therefore believes that the use of various protocols is a strength within Szymansky's design.

As for the remarks concerning the amended claims, they were reviewed but they are not deemed novel. As the new prior art explains, it is known that wireless networks are insecure for data transmissions. When important information is to be sent, such as the administration data claimed, it is obvious that it should not be sent out through a wireless transmission. In addition, they Szymansky art allows for routers and it is well known that routers can be setup to route such important information through more secure routes.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Azizul Choudhury whose telephone number is (571) 272-3909. The examiner can normally be reached on M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Valencia Martin-Wallace can be reached on (571) 272-6159. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AC

V. Martin-Wallace

VALENCIA MARTIN-WALLACE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3700